

La geolocalizzazione ai tempi del Covid-19: quali rischi per la privacy?

CHIARA DI SOMMA

Funzionario presso il Garante per la Protezione dei Dati Personali*

DAFNE CHILLEMI

Avvocato, Senior Associate dell'operating unit Intellectual Property, TMT & Digital Solution di PwC TLS Avvocati e Commercialisti

La situazione attuale

Nel contesto dell'attuale emergenza sanitaria, determinata dalla rapida diffusione del virus Sars-Cov-2 ("Covid-19" o "Coronavirus"), la tecnologia è stata annoverata tra le armi più efficaci per arginare l'epidemia.

In particolare, è stata valutata la possibilità di ricorrere a sistemi di sorveglianza sanitaria tramite l'utilizzo di tecniche di geolocalizzazione più nello specifico di contact tracing per tracciare i contagi da Covid-19 al fine, da un lato, di verificare il grado di ottemperanza alle misure di isolamento domiciliare e, dall'altro lato, di controllare in modo tempestivo il livello di esposizione al rischio delle persone e l'evoluzione dell'epidemia sul territorio nazionale. L'obiettivo di tali proposte è duplice: da una parte è chiaramente quello di tutelare la salute pubblica, evitando il collasso del sistema sanitario nazionale, già messo a dura prova dall'epidemia e, dall'altra, consentire all'economia nazionale, colpita duramente dal virus tanto quanto il settore sanitario, di ripartire.

* Le opinioni riportate in questo scritto sono espresse dall'autore a titolo esclusivamente personale e non riflettono necessariamente le posizioni dell'Autorità sull'argomento.



Su questo fronte, sembra innegabile il supporto che la tecnologia è in grado di fornire, basti solo pensare, per citare alcuni esempi, alle potenzialità di strumenti quali il tracciamento delle celle telefoniche, le reti wi-fi, i *bluetooth beacons* e la tecnologia Gps.

Tuttavia, è bene ricordare come il combustibile primo ed irrinunciabile di tali soluzioni sia costituito dai dati personali e dunque è necessario domandarsi quali siano le ricadute concrete in termini di tutela della privacy degli interessati e quanto il diritto della *data protection* possa essere compreso in nome di altri rilevanti interessi pubblici, primo fra tutti la tutela del bene della salute delle persone.

Se è pure vero che per perseguire la tutela della salute pubblica il diritto alla protezione dei dati personali possa subire (in casi di eccezionale gravità) delle compressioni, il Garante per la Protezione dei Dati Personali (il **Garante Privacy**) ha ricordato come le stesse debbano avvenire nel rispetto dei principi fondamentali stabiliti a tutela della democrazia, del principio di proporzionalità¹, e delle norme poste a tutela della privacy stessa.

In questa sede si desidera anticipare alcune riflessioni su di un tema che, per la sua attualità e complessità, sarà successivamente oggetto di approfondimento nel numero speciale di Privacy& di prossima pubblicazione.

Il quadro normativo

Preliminarmente, risulta utile chiarire cosa si intende quando si parla di “geolocalizzazione”.

Il termine fa riferimento al trattamento di dati personali che consentono l’individuazione della posizione geografica dell’interessato raccolti, ad esempio, tramite sistemi di *Global Positioning System* (GPS).

Ai sensi dell’articolo 2 della Direttiva 2002/58/CE del Parlamento Europeo e del Consiglio del 12 luglio 2002 relativa al *trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche* (la c.d. **direttiva e-privacy**) per “dati relativi all’ubicazione” si intende “ogni dato trattato in una rete di comunicazione elettronica che indichi la posizione geografica dell’apparecchiatura terminale dell’utente di un servizio di comunicazione elettronica accessibile al pubblico” (art. 2, par. 1 lett. c)).

Il Regolamento (UE) 2016/679 (il **GDPR** o il **Regolamento**) considera, invece, i dati relativi all’ubicazione come elementi identificativi di una singola

¹ P. Russo, *Un’app per la salute grazie a precise deroghe alla privacy – Intervista ad Antonello Soro*, in La Stampa, 25 marzo 2020, disponibile al seguente indirizzo: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9298389>



persona, conferendovi un rilievo particolare nelle complesse operazioni di profilazione nonché nei processi automatizzati (tra i quali potrebbe rilevare appunto la geolocalizzazione) volti alla valutazione di determinati aspetti relativi a una persona fisica (artt. 4, n. 1) e 22, cons. 71 e 72).

Inoltre, tanto il GDPR quanto la Direttiva e-privacy richiedono che il trattamento di dati personali relativi all'ubicazione trovi il proprio fondamento di liceità nel consenso dell'interessato².

Tuttavia – come ricordato anche nelle recenti dichiarazioni dello *European Data Protection Board* (lo **EDPB**) – l'attuale cornice normativa, dando voce all'articolo 52 della Carta dei diritti fondamentali dell'unione Europea, consente al legislatore nazionale di stabilire disposizioni limitative della privacy laddove costituiscano “una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica”³. Analogamente, l'articolo 23 del GDPR consente di limitare la portata di taluni obblighi e diritti, ivi inclusi i principi cardine applicabili al trattamento, “qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare” (...) “importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale”.

Nel contesto emergenziale, in Italia, l'articolo 14 del Decreto legge n. 14 del 9 marzo 2020 ha previsto la possibilità per i soggetti partecipanti al sistema di protezione civile di trattare dati personali sensibili o giudiziari per le finalità di contrasto all'epidemia e di relativa prevenzione ed assistenza sanitaria⁴. Tale disposizione non autorizza, tuttavia, il tracciamento degli interessati restando necessaria una norma *ad hoc* che possa costituire la base giuridica

² Si veda ad esempio, sul punto, Regolamento (UE) 2016/679, Considerando 71, Considerando 75, Articolo 6, Articolo 13, Direttiva 2002/58/CE, Articolo 9, D.Lgs. 196/2003 e s.m.i.

³ Direttiva 2002/58/CE, articolo 15.

⁴ L'art. 14 del decreto legge n. 14 del 9 marzo 2020 prevede che: “fino al termine dello stato di emergenza deliberato dal consiglio dei ministri in data 31 gennaio 2020, per motivi di interesse pubblico nel settore della sanità pubblica e, in particolare per garantire la protezione dall'emergenza sanitaria [...] le strutture pubbliche e private che operano nell'ambito del Servizio sanitario nazionale e i soggetti deputati a monitorare e a garantire l'esecuzione delle misure disposte ai sensi del decreto legge 23 febbraio 2020 n.6 anche allo scopo di assicurare la più efficace gestione dei flussi e dell'interscambio dei dati personali, possono effettuare trattamenti, ivi inclusa la comunicazione tra loro, dei dati personali, anche relativi agli articoli 9 e 10 del regolamento (UE) 2016/679, che risultino necessari all'espletamento delle funzioni attribuitegli nell'ambito dell'emergenza determinata dal diffondersi del COVID-19”.



per il trattamento dei dati sotteso alle iniziative di *contact tracing*⁵ e che, soprattutto, dotata di efficacia temporalmente limitata, fornisca adeguate garanzie in conformità al principio di proporzionalità⁶.

Riassumendo, quindi, il monitoraggio dei cittadini per finalità di contrasto del contagio risulterebbe lecito a condizione che i) gli Stati membri prevedano le deroghe con un atto avente forza di legge e ii) le modalità derogatorie siano in ogni caso compatibili con una società democratica⁷.

In tale contesto, secondo quanto affermato dal Garante Privacy, il trattamento dei dati personali deve, in ogni caso, costituire il risultato del bilanciamento tra l'invadere il meno possibile la sfera personale e l'adozione di misure che siano però sufficienti ai fini di prevenzione⁸.

Da monito anche le parole della presidente dell'EDPB, Andrea Jellinek, secondo la quale le autorità pubbliche dovrebbero cercare, in ogni caso, di trattare tali dati in modo anonimo e aggregato, così da non consentire l'identificazione, anche successiva, degli individui cui si riferiscono⁹.

⁵ O. POLLICINO E G. DE GREGORIO, *Emergenza Coronavirus, fin dove può spingersi il tracciamento degli smartphone?*, in www.federprivacy.org, 20 marzo 2020, disponibile al seguente indirizzo: <https://www.federprivacy.org/informazione/punto-di-vista/item/1344-emergenza-coronavirus-fin-dove-puo-spingersi-il-tracciamento-degli-smartphone>; A. IANNUZZI, *Soro: sì al tracciamento dei contatti ma con un decreto temporaneo*, *Intervista ad Antonello Soro*, in *La Repubblica*, 26 marzo 2020, disponibile al seguente indirizzo: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9299193>.

⁶ A. IANNUZZI, *Soro: sì al tracciamento dei contatti ma con un decreto temporaneo*, *Intervista ad Antonello Soro*, in *La Repubblica*, 26 marzo 2020, disponibile al seguente indirizzo: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9299193>; A. SORO, *Tracciamento dei contagi coronavirus, ecco i criteri da seguire*, in www.agendadigitale.eu, 29 marzo 2020, disponibile al seguente indirizzo: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9301470>; si vedano anche EUROPEAN DATA PROTECTION SUPERVISOR, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf; EUROPEAN DATA PROTECTION SUPERVISOR, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, disponibili qui: https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf

⁷ F. PIZZETTI, *Pizzetti: "A rischio la libertà dei cittadini, urgente un intervento giuridico"*, in www.agendadigitale.eu, 23 marzo 2020, disponibile al seguente indirizzo: <https://www.agendadigitale.eu/sicurezza/privacy/pizzetti-a-rischio-le-liberta-dei-cittadini-urgente-un-intervento-giuridico/>.

⁸ A. SORO, *Tracciamento dei contagi coronavirus, ecco i criteri da seguire*, in www.agendadigitale.eu, 29 marzo 2020, disponibile al seguente indirizzo: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9301470>.

⁹ EUROPEAN DATA PROTECTION BOARD, *Statement on the processing of personal data in the context of the COVID-19 outbreak*, del 19 marzo 2020, disponibile al seguente indirizzo: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldata-andcovid-19_en.pdf.



La soluzione italiana: una App per tracciare i contagi

Una volta analizzato il quadro normativo, vediamo, a livello nazionale, quali sono le “mosse” intraprese dal Governo e dagli operatori, pubblici e privati. La possibilità di ricorrere all'utilizzo della geolocalizzazione nella lotta al Covid-19 è salita alla ribalta della cronaca nazionale (oltre che mondiale) a seguito dell'iniziativa assunta dalla Regione Lombardia, quando il vicepresidente della Regione e assessore per la ricerca Fabrizio Sala, di concerto con l'assessore al Welfare Giulio Gallera, hanno reso noto di aver analizzato gli spostamenti “da cella a cella” dei telefoni cellulari degli abitanti per comprendere la quantità, la modalità e la frequenza di spostamento degli stessi all'interno del territorio monitorato.

La Regione ha così acquisito dati (che ha tenuto immediatamente a precisare raccolti in forma anonima e aggregata) con l'ausilio delle compagnie di telecomunicazioni Vodafone e Tim¹⁰.

In parallelo, sempre più forti si stanno facendo le istanze di soggetti, pubblici e privati, di spingere l'analisi dei dati oltre l'“anonimato”, al fine di avere un monitoraggio molto più accurato in merito all'espansione del virus ed alle concrete modalità di contagio.

La maggior parte delle proposte prevedono, sulla falsariga del modello adottato in Corea del Sud, l'uso di app mobili che, con l'ausilio della tecnologia GPS o Bluetooth, consentono la creazione di una vera e propria mappa del contagio. Il Governo italiano, perciò, ha deciso di intervenire con un piano che ha previsto inizialmente una “call” per la sottoposizione di soluzioni tecnologiche idonee a contenere l'epidemia¹¹.

Lo step successivo del “piano” si è concretizzato nella istituzione – con decreto a firma del Ministro per l'Innovazione tecnologica e la digitalizza-

¹⁰ M. PENNISI, *Coronavirus, come funzionano il controllo delle celle e il tracciamento dei contagi. Il Garante: “Non bisogna improvvisare”* intervista ad Antonello Soro, in *Il Corriere della Sera*, 18 marzo 2020, disponibile al seguente indirizzo: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9294705>.

¹¹ Il 23 marzo scorso, il Governo ha promosso l'iniziativa “*Innova per l'Italia*”, una “call” rivolta a soggetti privati e pubblici, con l'obiettivo di individuare le migliori soluzioni digitali – concrete, già realizzate e idonee ad una rapida implementazione – che utilizzino sistemi di *data analytics*, intelligenza artificiale e *big data*. Si tratta, in particolare, di applicazioni (“app”) di c.d. telemedicina e assistenza domiciliare ai pazienti contagiati dal virus SARS – CoV – 2 (“Covid – 19”) quali, ad esempio, *chatbot* che consentano alle persone l'automonitoraggio delle proprie condizioni di salute, nonché app che utilizzino tecniche di geolocalizzazione con finalità di monitoraggio del rischio di contagio, aventi requisiti di interoperabilità con sistemi aziendali e/o regionali e modalità c.d. *user friendly* in merito all'identificazione, l'autenticazione, l'informativa e l'eventuale consenso informato rilasciato dall'utente.



zione, di concerto con il Ministero della Salute, l'Istituto Superiore di Sanità e l'Organizzazione Mondiale della Sanità – di una *task force* di 74 esperti¹² per l'esame delle soluzioni tecnologiche *data driven* idonee a supportare il Governo nella definizione delle politiche di contenimento dell'epidemia¹³. Tra le proposte al vaglio della *task force*, interessante risulta l'app *Pj19*, ideata e progettata dalla società italiana Vetrya, in collaborazione con il Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNIT). L'applicazione, da installare su *smartphone*, consente di ricavare i dati sulla diffusione del Covid-19 attraverso un sistema di *mapping* basato su intelligenza artificiale¹⁴. I dati vengono poi forniti alle strutture competenti per l'analisi, senza passare per gli operatori di telecomunicazioni.

L'app *Private-Kit*, sviluppata dal *Massachusetts Institute of Technology* di Boston adotta, invece, una combinazione di tecnologia GPS e *Bluetooth*¹⁵. L'applicazione registra tutti gli spostamenti e li salva sulla memoria del telefono a intervalli di cinque minuti. L'accesso ai dati, conservati in maniera anonima e criptata, sarà consentito soltanto agli operatori sanitari, nel caso in cui l'interessato manifesti i sintomi del Coronavirus e si rechi in una struttura ospedaliera. I dati verranno poi caricati all'interno di un server che li aggrega, inviando, al contempo, un segnale a tutti gli utenti che utilizzano l'app. Infine, è stata elaborata una funzionalità che permette di incrociare i dati salvati sullo *smartphone* con quelli a disposizione del sistema sanitario e notifica all'utente se è entrato in contatto con una persona che è risultata positiva (sempre e rigorosamente in modo anonimo).

¹² I membri sono stati designati, dal Ministero della Salute, dall'Istituto Superiore di Sanità e dall'Organizzazione Mondiale della Sanità, dall'Autorità Garante della Concorrenza e del Mercato (AGCM), dall'Autorità per le Garanzie nelle Comunicazioni (AGCOM) e dal Garante per la Protezione dei Dati Personali (Garante Privacy). Gli stessi sono ripartiti in otto sottogruppi di lavoro, i quali, a loro volta, riporteranno le loro determinazioni al gruppo di valutazione finale composto dagli esperti delle autorità indipendenti AGCM, AGCOM e Garante Privacy, che si occuperanno della relazione conclusiva da sottoporre al vaglio del Ministro per l'innovazione tecnologica e la digitalizzazione.

¹³ MINISTRO PER L'INNOVAZIONE TECNOLOGICA E LA DIGITALIZZAZIONE, *Nasce la task force italiana per l'utilizzo dei dati contro l'emergenza Covid-19*, in www.innovazione.gov.it, 31 marzo 2020, disponibile al seguente indirizzo: <https://innovazione.gov.it/nasce-la-task-force-italiana-per-l-utilizzo-dei-dati-contro-l-emergenza-covid-19/>.

¹⁴ A. DINI, *Data tracing, soluzione made in Italy a base di intelligenza artificiale*, in www.agendadigitale.eu, 25 marzo 2020, disponibile al seguente indirizzo: <https://www.corrierecomunicazioni.it/digital-economy/data-tracing-vetrya-in-campo-con-lai-a-prova-di-privacy/>.

¹⁵ E. SERRA, *Coronavirus, i tre italiani di "Private Kit": l'app del Mit che traccia i contagi*, 28 marzo 2020, disponibile al seguente indirizzo: https://www.corriere.it/cronache/20_marzo_28/coronavirus-tre-italiani-private-kit-l-app-mit-che-traccia-contagi-03c36c12-710d-11ea-a7a2-3889c819a91b.shtml.



La scelta delle soluzioni da implementare non può, in ogni caso, sottrarsi ad una preliminare valutazione in merito all'idoneità a conseguire gli obiettivi prefissati, in particolar modo tenendo a mente il principio di proporzionalità¹⁶.

Alcune regioni, come Lombardia¹⁷ e Umbria¹⁸, stanno già sperimentando delle soluzioni autonome.

In tale contesto, è lecito, tuttavia, domandarsi se la *task force* valuterà l'estensione di soluzioni locali (come quella lombarda) anche al resto del territorio (sulla falsa riga del modello spagnolo dell'app "Asistencia-Covid 19"), oppure deciderà di aprire a soluzioni diverse, magari ancor più innovative, sempre di impronta pubblicistica. Del resto, data l'estrema delicatezza del tema, potrebbe apparire più cautelativa l'adozione di uno strumento unico e uniforme su tutto il territorio nazionale, anche al fine di scongiurare soluzioni lesive del principio di eguaglianza in senso sostanziale, che potrebbero ripercuotersi negativamente sui diritti delle persone residenti in specifiche zone del paese. Lo stesso Garante Privacy incoraggia fortemente l'adozione di una soluzione unica a livello nazionale, in modo da garantire che i dati siano raccolti e trattati da un'autorità pubblica¹⁹: i soggetti privati coinvolti, oltre a possedere requisiti idonei di affidabilità e trasparenza, dovrebbero ricoprire esclusivamente il ruolo di "collettori" di un patrimonio informativo da affidare esclusivamente alla pubblica autorità²⁰.

Tuttavia, non è da escludere che la *task force* possa optare per un modello alternativo, simile alla soluzione sud coreana, improntato alla gestione privatistica della raccolta dei dati tesi al monitoraggio dell'epidemia tramite diverse app realizzate da privati fra le quali i cittadini possono liberamente scegliere.

¹⁶ A. SORO, *Tracciamento dei contagi coronavirus, ecco i criteri da seguire*, in www.agendadigitale.eu, 29 marzo 2020, disponibile al seguente indirizzo: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9301470>.

¹⁷ M. PENNISI, S. RAVIZZA, *AllertaLOM, l'app di regione Lombardia per mappare gli infetti: ecco come funziona*, in *Il Corriere della Sera*, sezione Tecnologia, 1 aprile 2020, disponibile al seguente indirizzo: https://www.corriere.it/tecnologia/20_aprile_01/app-mappare-infetti-debutta-lombardia-governo-chiama-74-esperti-e4964616-73e6-11ea-b181-d5820c4838fa.shtml.

¹⁸ E. MARIONI, *Come funziona l'app per tracciare i contatti testata dall'Umbria*, in www.agi.it, 22 marzo 2020, disponibile al seguente indirizzo: <https://www.agi.it/cronaca/news/2020-03-22/covid-19-umbria-app-tracciamento-7763334/>.

¹⁹ P. RUSSO, *op. cit.*

²⁰ A. CATALETA, G. FAGIOLI, *Covid-19: l'app per monitorare i contagi serve ora, ma sia pubblica*, in www.agendadigitale.eu, 30 marzo 2020, disponibile al seguente indirizzo: <https://www.agendadigitale.eu/sicurezza/privacy/covid-19-lapp-per-monitorare-lepidemia-serve-ora-ma-sia-pubblica/>.

Conclusioni

Sicuramente il diritto alla salute e il diritto alla privacy devono convivere in armonia fra loro e la loro convivenza non può che fondarsi sul reciproco rispetto dei principi posti a fondamento di entrambe le normative.

Non a caso, l'EDPB – in una lettera indirizzata a Roberto Viola, Direttore Generale di DG Connect (l'ente della Commissione Europea che si occupa, tra l'altro, di economia digitale, ricerca e innovazione) – ribadisce con forza alcuni punti fondamentali che in questa sede appare opportuno riassumere²¹:

- il GDPR incorpora già tutti gli strumenti per tutelare i dati personali e per fronteggiare al contempo anche una crisi sanitaria come quella attuale;
- i dati anonimizzati non sono soggetti all'applicazione del GDPR, ma l'anonimizzazione deve essere effettiva. Non basta, infatti, rimuovere i dati identificabili come il numero di telefono o l'IMEI;
- anche se i dati sono anonimizzati, la loro sicurezza e confidenzialità devono essere sempre garantite;
- è opportuno restringere il numero di soggetti terzi coinvolti nel trattamento, verificando che forniscano adeguate garanzie di sicurezza, soprattutto quando si fa riferimento alle compagnie telefoniche, incaricate del trasferimento dei dati personali agli enti pubblici o privati;
- i dati devono essere cancellati non appena l'emergenza sarà terminata. Le app utilizzate per il monitoraggio, infatti, rappresentano una soluzione straordinaria e come tale devono essere trattate; non devono pertanto considerarsi leciti usi volti a perseguire scopi ulteriori rispetto a quelli della raccolta;
- la trasparenza verso i cittadini e il coinvolgimento stretto del Garante sono i moniti più importanti.

Solo in questo modo sarà possibile sfruttare appieno i vantaggi che la tecnologia può offrire in un contesto di emergenza come quello odierno, senza però cedere alla tentazione della “*scorciatoia tecnologica*”, come puntualizzato da Antonello Soro, presidente del Garante Privacy, evitando quindi processi di monitoraggio indiscriminato di massa²².

²¹ EUROPEAN DATA PROTECTION SUPERVISOR, *Monitoring spread of COVID-19*, lettera di risposta al Directorate Generale for Communications Networks, Content and Technology presso la Commissione Europea, disponibile al seguente indirizzo: https://edps.europa.eu/sites/edp/files/publication/20-03-25_edps_comments_concerning_covid-19_monitoring_of_spread_en.pdf.

²² M. PENNISI, *op. cit.*